Received: 15 January 2021 | Revised: 13 April 2021 | Accepted: 16 April 2021

DOI: 10.1002/spe.2983

SPECIAL ISSUE PAPER

WILEY

NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates

Amal Abid[1] | **Saoussen Cheikhrouhou**[1,2] | **Slim Kallel**[1,2] | **Mohamed Jmaiel**[1,2]

[1]ReDCAD, National Engineering School of Sfax, University of Sfax, Sfax, Tunisia

[2]Digital Research Center of Sfax, Sfax, Tunisia

Correspondence
Amal Abid, ReDCAD, National Engineering School of Sfax, University of Sfax, Sfax BP. 1173, 3038, Tunisia.
Email: amal.abid@redcad.org

Abstract

The COVID-19 pandemic has emerged as a highly transmissible disease which has caused a disastrous impact worldwide by adversely affecting the global economy, health, and human lives. This sudden explosion and uncontrolled worldwide spread of COVID-19 has revealed the limitations of existing health-care systems regarding handling public health emergencies. As governments seek to effectively re-establish their economies, open workplaces, ensure safe travels and progressively return to normal life, there is an urgent need for technologies that may alleviate the severity of the losses. This article explores a promising solution for secure Digital Health Certificate, called NovidChain, a Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates issuing and verifying. More precisely, NovidChain incorporates several emergent concepts: (i) Blockchain technology to ensure data integrity and immutability, (ii) self-sovereign identity to allow users to have complete control over their data, (iii) encryption of Personally Identifiable Information to enhance privacy, (iv) W3C verifiable credentials standard to facilitate instant verification of COVID-19 proof, and (v) selective disclosure concept to permit user to share selected pieces of information with trusted parties. Therefore, NovidChain is designed to meet a high level of protection of personal data, in compliant with the GDPR and KYC requirements, and guarantees the user's self-sovereignty, while ensuring both the safety of populations and the user's right to privacy. To prove the security and efficiency of the proposed NovidChain platform, this article also provides a detailed technical description, a proof-of-concept implementation, different experiments, and a comparative evaluation. The evaluation shows that NovidChain provides better financial cost and scalability results compared to other solutions. More precisely, we note a high difference in time between operations (i.e., between 46% and 56%). Furthermore, the evaluation confirms that NovidChain ensures security properties, particularly data integrity, forge, binding, uniqueness, peer-indistinguishability, and revocation.

KEYWORDS

Blockchain, COVID-19 pandemic, digital health certificate, GDPR, KYC, privacy self-sovereignty, W3C verifiable credentials

1 | INTRODUCTION

Governments worldwide are still dealing with COVID-19 pandemic, an outbreak of the SARS-CoV-2 virus, which continues to cause immense damage on the lives of citizens and the economies of more than 190 countries, causing more than 82 million cases and over 1.8 million deaths worldwide at the time of writing this article (December 2020).

Besides the COVID-19 mitigation measures, the economy reopening strategy has become the main concern of each government, business, and individual. One of the challenges for governments and public authorities is to manage their economies effectively, open workplaces, authorize travel, as well as preventing further waves of infection. In fact, a high percentage of service sector companies might not reopen again due to financial fall. They desperately wish a solution that preserves a healthy environment to keep their business open and their customers satisfied. As governments attempt to progressively return to normal life, there is an urgent need for technologies that may alleviate the severity of the losses.

Different technological solutions are considered, particularly movement documents and traceability apps,[1-3] but all are vulnerable to fraud and falsification and may influence on basic liberties or be socially unacceptable. More precisely, due to the nature of traceability apps, public worry on privacy issues has been an obstacle to the existing solutions.[4-6] In particular, personal data privacy and confidentiality are threatened due to Google/Apple[7] contact tracing features. Moreover, in Bluetooth-based traceability Apps, user device is required to remain in an active broadcasting state, hence draining its battery. Meanwhile, the Bluetooth technology has security issues such as vulnerable wireless interface and physical hardware identification and exposure. Moreover, there is a high risk of replay attacks to the traceability network, which may cause a massive scale of panic to the public.[6]

A promising solution consists of using the so-called "health certificate"/ "immunity passport"/ "risk-free certificate" or any other highly secure health document. The general idea is that a COVID-19 test or vaccine proof could serve as the basis for a certificate that liberates an individual from the most restrictive government regulations. It aims to allow anyone, who obtained an approved PCR/Antibody test result or has been vaccinated, to receive a certificate, in a digital but printable format which is tamper-proof and universally verifiable. Consequently, this health certificate could allow public authorities to control access to critical or sensitive facilities, such as hospitals, retirement homes, schools, government offices, workplaces and companies, while taking in consideration the remaining uncertainties about the virus, changing health policies and the validity period of the test result. Moreover, compared with traceability apps, the health certificate is privacy-preserver and is only scanned at the time of crossing checkpoints (i.e., Airports, Hospitals, Schools), hence saves the user battery, since it can be used in offline mode and does not consume energy.

Some countries such as China, Chile, Estonia, United States, United Kingdom, Italy, Germany, and France have already reported plans to trial such certificates.[8-12] Unfortunately, these solutions, trialed and implemented by governments,[9-12] provide few technical details and cannot be fully understood or reviewed. It is, however, well known that some of them are centralized[9] or rely on third parties,[11] thus resulting in security and privacy-preserving issues.

In line of the interest already shown by some governments, and the occurrence of a number of commercial solutions,[13,14] an academic consideration of COVID-19 health certificates is needed. In particular, it is essential to provide detailed technical solutions, and to recognize current limitations, so that healthcare authorities can be accurately informed. Moreover, there are a high number of developing countries that have no technical nor economic capacity to win this fight. How can we harness the technology and solutions to boost these countries through a global standard?

To help deal with this worldwide health pandemic, the Blockchain technology[15,16] can perform an essential role not only in disease alleviation but also in facilitating the enforcement of governmental regulations and guidelines, while keeping trust between all stakeholders. Indeed, the emergent Blockchain technology, which is a distributed, immutable, and tamper-proof ledger database with global computational infrastructure (i.e., smart contracts), has the potential to provide efficient COVID-19 solutions based on high levels of accuracy and trust thanks to its key properties of transparency, integrity, and resilience.[17]

Accordingly, we propose, in this article, a Blockchain-based privacy-preserving health certificate platform, named NovidChain, for COVID-19 test/vaccine certificates issuing and verifying. NovidChain aims to curb the propagation of COVID-19 while ensuring privacy requirements such as General Data Protection Regulation (GDPR) and Know Your Customer (KYC), and guaranteeing the user's self-sovereignty. The proposed approach will not only be applied to COVID-19 tests but also to COVID-19 vaccines, as they have become available in some countries. We think that NovidChain could be the cornerstone of a future COVID-19 secure vaccine certificate Worldwide in particular for travelling since COVID-19 "vaccine passports" will be required for 2021 travels.[18]

The main contributions of this article, provided with the proposed solution, are:

1. *Privacy preservation*: NovidChain relies on an off-chain InterPlanetary File System-IPFS storage[19] to store encrypted user's personal data including COVID-19 results. Only the IPFS hash is stored on-chain, allowing sensitive information to never be revealed to others scanning the Blockchain.
2. *GDPR-compliance*: NovidChain is GDPR-Compliant since it relies on solid common standards for data protection such as W3C verifiable credentials (VC),[20] ERC1056 Lightweight Ethereum Identity,[21] and JSON Web Tokens (JWT),[22] and thus users can be sure that they are in control of their personal information.
3. *Self-sovereignty*: In NovidChain, users are the owner of their identity and have complete control over personal data including issued COVID-19 certificate. Moreover, NovidChain supports selective disclosure concept that permits users to share selected pieces of information with chosen trusted parties.
4. *KYC-compliance*: NovidChain is KYC-Compliant since it verifies the identity of different users before onboarding them. This would allow more secure interactions and control over the data that accumulates around a specific identity and would serve for collecting true information of the population's state of immunity in our case. Therefore, the proposed approach would serve as the basis for real-time monitoring of the population's health status and of the deconfinement evolution and the management of the pandemic.
5. *Integrity*: Since the hash of the data is stored immutably in the Blockchain, we can verify the integrity of the COVID-19 data by comparing the hash value of the data shared by the user with that stored in the Blockchain.

To prove the feasibility and validity of the proposed NovidChain platform, this article provides a detailed technical description, a proof-of-concept implementation, different experiments, and a comparative evaluation. The evaluation shows that NovidChain provides better financial cost and scalability results compared to existing solutions. Particularly, we note a high difference in time between operations (i.e., between 46% and 56%). Furthermore, security properties evaluation confirms that these may be satisfied in practice. This would allow us to consider NovidChain as an open initiative which is designed to reach the highest level of personal data protection, thus protecting both the population and the user's right to privacy.

The rest of this article is organized as follows. Section 2 introduces some concepts upon which NovidChain is built. Section 3 provides a high level overview, while Section 4 explains how NovidChain ensures privacy. Section 5 presents NovidChain in action. Section 6 provides a proof-of-concept implementation, while Section 7 performs validations and experiments. Section 8provides a comparative evaluation. Section 9 reviews the related work. Section 10 explores new aspects to enhance NovidChain platform, and Section 11 concludes this work with future work.

2 | BACKGROUND

This section introduces the main concepts and definitions related to Blockchain, W3C VC, and uPort.

2.1 | Blockchain

Introduced a decade ago by an anonymous contributor under the pseudonym of Satoshi Nakamoto,[15] the Blockchain technology has immense potential to evolve a variety of sectors including government, finance, industry, education, and health. The Blockchain represents a continuously growing tamper-resistant ledger that maintains a permanent record of all the transactions in a distributed, time-stamped and secure way over a peer-to-peer network. Derived from various well-known core technologies, including cryptographic hash function, cryptographic digital signature, and distributed consensus, it affords some key functionalities such as data persistence, transparency, anonymity, fault-tolerance, integrity, and execution in a trustless environment.

More recently, the introduction of smart contracts has transformed the Blockchain from a pure distributed database to a hybrid distributed storage and computing platform. The term of smart contract, proposed in Reference 16, designates a Turing-complete program that checks and executes a set of rules over a Blockchain network. More precisely, it is a digital protocol which implements terms and promises predefined by parties who proceed to an agreement. The first platform enabling smart contracts execution is called Ethereum. It makes this possible through a computational language, named

Solidity, that stores smart contract programs in the form of Ethereum Virtual Machine (EVM) bytecode, and it enables transactions as function calls into that code/program.

The main Blockchain properties are:

1. *Immutable Ledger through hash cryptography*: Blockchain is a distributed ledger that stores data in an ordered chain of blocks and is shared, replicated, and synchronized among the participants of a P2P network.

   The blocks are divided into block-data and an associated block-header that stores the SHA-256 hash of the data. Furthermore, each block includes the hash of the previous block-header in its own header in order to reinforce and confirm the data of its preceding block (see Figure 1). This property constitutes the cryptographic link between blocks which makes it impossible to retrospectively modify data in a single block without modifying the subsequent blocks of the data in the chain. For this reason all participants can examine the Blockchain without being able to tamper it.
2. *P2P Network*: If a hacker now attempts to maliciously attack any entry in a specific block of the Blockchain, the cryptographical link of the chain will be invalidated. However, if the hacker has enough time as well as the computing power to change the hashes of all successive blocks and update them with new information, he/she would have to attack at least 51% of the computers in the network simultaneously, and perform it within a few seconds to accomplish data tampering. This will be very hard to carry out, for not saying impossible.
3. *Consensus*: The nodes in a Blockchain network are responsible for storing track of all transactions and executing the code of smart contracts. To maintain a single consistent state of the system, all nodes in the network need to achieve consensus (agreement) on the validity and order of broadcasted transactions by voting on them. While there are many different consensus protocols, currently the most common types for a Blockchain are Proof-of-Work (PoW) and Proof-of-Stake (PoS). The advantage of these two over traditional mechanisms, such as Practical Byzantine Fault Tolerance (PBFT), is that they allow a trustless, open network where everyone can join without the need to hold a list of permissioned nodes authorized to vote for a certain system state.

Regarding the control of permissions, current Blockchain implementations belong to three categories: public, consortium, and private. In the case of a public Blockchain, everyone can read and maintain the ledger, that is, there is no membership mechanism in place. While, in a consortium Blockchain, a predefined consortium of peers is in charge of conserving the ledger. In a private Blockchain network, a single entity controls the whole system.

2.2 | W3C verifiable credentials

The W3C VC[20] is a standard which is specifically designed to deal with digital credentials, claims and certifications in a secure and privacy-preserving manner. The main ideas are based on existing well-known concepts such as the Public Key Infrastructure (PKI). This latter underlies the public/private key pairs model that simplifies digital signatures in

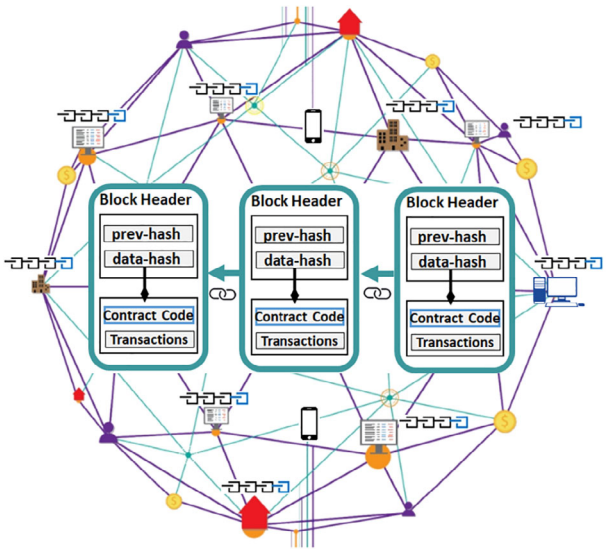


FIGURE 1 Illustration of the blockchain [Colour figure can be viewed at wileyonlinelibrary.com]

widespread use today. Moreover, the W3C VC is designed to standardize the definitions of document formats that enable them to be machine-readable and communicable, and to generalize PKI, which are generally costly and highly centralized. The generalization moves to a decentralized/distributed registry for cryptographic keys, typically (but not necessarily) residing in a Blockchain because this allows every public key to have its own unique address: such an address is known as a Decentralized Identifier (DID).

The different roles and information flows of the W3C VC model are presented in Figure 2. The subject should create globally unique identifiers through a verifiable data registry. The holder asks the issuer to produce a VC by linking properties to identifiers. The holder is usually, but not always, the subject of the VC they are maintaining. For example, a parent may maintain a child's VCs. The issuer verifies the holder's identifiers and the properties, and its right to hold the subject's VC, and then issues the VC. The holder should maintain the issued VC. Finally, the holder can bring a verifiable presentation of his/her credentials to the verifier. In this model, VC issuers do not know the identities of verifiers, which presents a considerable evolution from current identity management systems.

2.3 | uPort

uPort[23] is a self-sovereign identity and user-centric data platform built on Ethereum Blockchain. The uPort infrastructure is constituted of a mobile app holding a self-sovereign wallet, an authentication mechanism for modern web applications/decentralized applications, and associated developer's libraries.

Figure 3 presents the general architecture of uPort identity management system, and illustrates how it works.[23] In uPort, any user/app can interact with an "Application Contract" for identity related information. This operation affects two main contracts: a "Proxy Contract" that acts as a universal and permanent user identifier, and a "Controller Contract" that provides identity access control logic. The app interacts with the "Proxy Contract" through the "Controller Contract" which sends a request to the corresponding application. As a permanent identifier on the Blockchain, the "Proxy Contract" interacts with all application contracts and creates a layer between the user's private key (in the digital wallet) and application contracts. To establish this communication, uPort uses a standard RPC interface provided by Infura,[24] which presents an infrastructure to communicate with the Ethereum network. Besides, a user can send a transaction without owing any Ether in his/her wallet, by sending it to the uPort Sensui server which then supplies suitable Ether to pay the

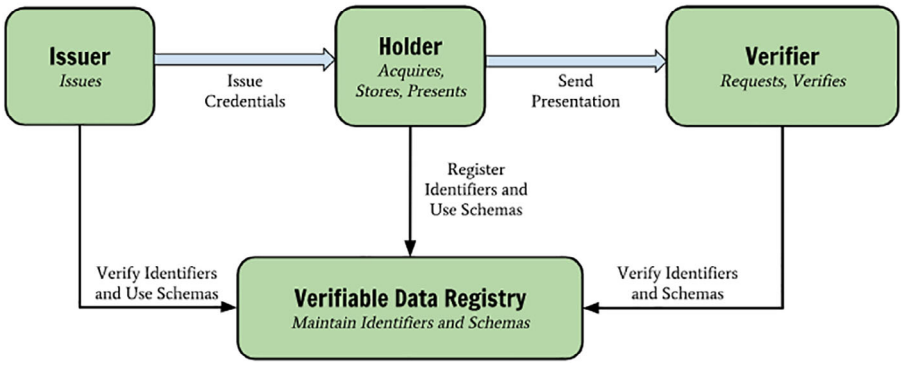


FIGURE 2 Main roles and workflow in W3C verifiable credentials[20] [Colour figure can be viewed at wileyonlinelibrary.com]

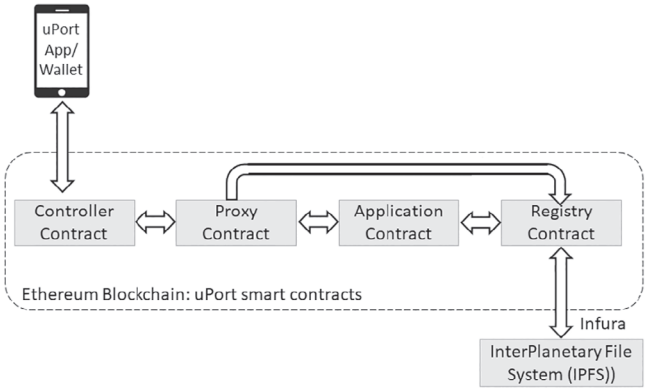


FIGURE 3 uPort general architecture

transaction fee. Finally, the uPort identity related data can be encrypted and stored off-chain (e.g., InterPlanetary File System [IPFS][19]). This can be achieved by creating a cryptographic link to an external data structure using a "Registry Contract," which can only be updated by the "Proxy Contract." Here, uPort requires Infura interface to communicate with the off-chain network.

It should be noted that uPort relies on W3C VC standard, and encloses further mechanisms helping to reduce the exposure of personal information by users, such as the concept of Selective Disclosure. Through this concept, the user is able to select some elements of his/her VC to share with a verifier, without revealing the rest. This represents certainly a relevant step forward in ensuring the users' right to the protection of personal data.

3 | NOVIDCHAIN HIGH LEVEL OVERVIEW

This section provides a high level overview of the proposed NovidChain approach by presenting the NovidChain's proposed infrastructure, involved actors, and the main process to achieve a secure COVID-19 certificate solution.

NovidChain is a Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificate issuing and verifying. The proposed platform facilitates instant verification of tamper-proof COVID-19 test/vaccine and thus helping in restraining the COVID-19 propagation, while protecting the user's right to privacy. The general idea is that a secure COVID-19 certificate would serve as a proof that a person has obtained a negative test result, recovered from COVID-19 or been vaccinated against COVID-19. This would simplify safe free movement and liberate an individual from most restrictive government regulations. Besides, this secure COVID-19 certificate could help public authorities to control access to critical or sensitive facilities, such as hospitals, retirement homes, airports, schools, government offices, and workplaces.

3.1 | Infrastructure and involved actors

This subsection presents the proposed NovidChain infrastructure as illustrated in Figure 4. First, we introduce the different components of the infrastructure, then we enumerate the involved actors.

3.1.1 | Infrastructure components

In order to ensure an effective solution, an appropriate infrastructure has to be built (Figure 4). The proposed NovidChain infrastructure includes two main components: a private permissioned Blockchain and an off-chain storage which are described as follows.

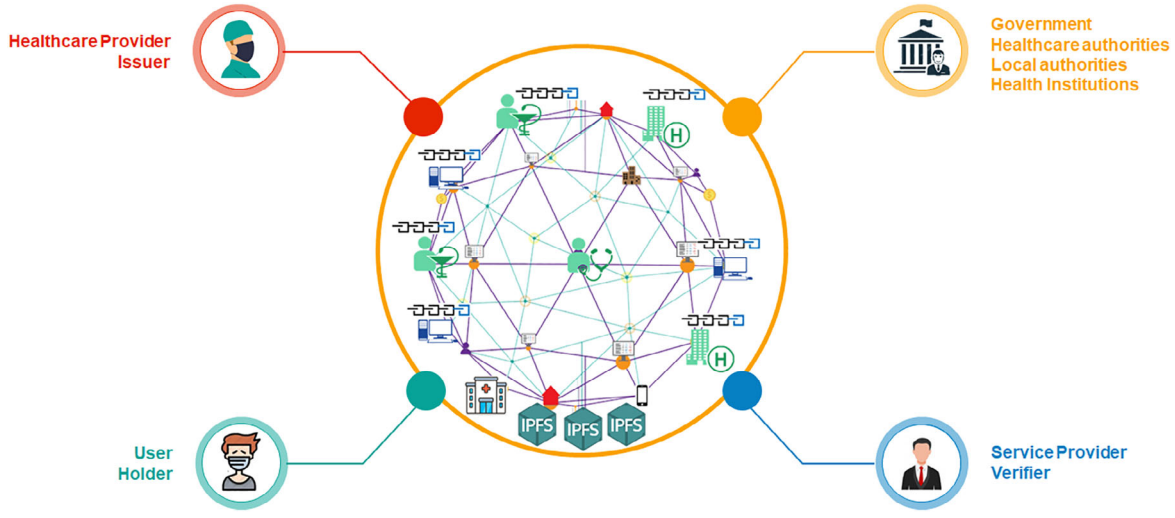


FIGURE 4 NovidChain infrastructure and involved actors [Colour figure can be viewed at wileyonlinelibrary.com]

- *Private permissioned Blockchain*: The proposed infrastructure relies on Ethereum private permissioned Blockchain to address privacy issues of such COVID-19 health environment. This allows only authorized users to access to the system by verifying their cryptographic keys. The Blockchain serves as a tamper-proof verifiable data registry.
- *Off-chain storage*: An off-chain InterPlanetary File System-IPFS storage[19] is used to store user's personal data including COVID-19 results. Only the IPFS hash is stored on-chain, allowing sensitive information to never be revealed to others scanning the Blockchain. More precisely, encrypted COVID-19 data can be stored separately of the Blockchain in an off-chain storage (e.g., private network of nodes, which are joint or disjoint from the Blockchain network), while the Blockchain stores only a pointer to encrypted data resided on this off-chain storage. It is strictly speaking Personally Identifying Information are anchored to the Blockchain rather than created on the Blockchain. This enables NovidChain to ensure GDPR privacy requirements, since IPFS hashes act as control pointers to encrypted GDPR-sensitive data.

3.1.2 | Involved actors

The principal roles of the involved actors are described as follows.

- *Government/health authorities and health institutions*
  Government and health authorities grant authorization to perform COVID-19 test/vaccine and issuing certificates. They regulate the supply of tests/vaccines and distribute them to health institutions. Meanwhile, they determine which tests are qualified for the proof of immunization, and they authorize who is allowed to get the vaccine according to prioritization strategies. On the other side, government and local authorities assign authorization to service providers to perform COVID-19 certificates verification.
- *Healthcare providers/issuers*
  Healthcare providers/issuers (i.e., Doctors, Nurses) operate and control COVID-19 tests/vaccines. These issuers must be approved by healthcare authorities and identifiable in a transparent manner, in order to guarantee safety and traceability. Besides, they treat the tested/vaccinated cases and record the COVID-19 results on the Blockchain.
- *Users/holders*
  People who have been vaccinated, received a valid antibody test, or a negative PCR test could work and access a public place. They must bring an official physical document such as Passport or ID card to identify themselves and obtain a digital ID. This digital ID operates through providing a unique QR code, based on Blockchain address account and associated to personal data such as name, the official physical ID number and the security code. When a person needs to prove his/her health status, Digital ID and physical ID are required for identification.
- *Service providers/verifiers*
  Service providers (i.e., employer, retirement home, school, airport, etc.) verify and confirm issued COVID-19 certificates by scanning the QR code and checking digital signatures. These verifiers must be authorized by the local authorities and transparently identifiable, to ensure security and traceability.

3.2 | Main process for NovidChain

Figure 5 illustrates the main process for the proposed NovidChain approach, which is described as follows.

1. *Healthcare provider and service provider registration*
   First of all, a healthcare provider, which would like to be an authorized COVID-19 certificate Issuer, must create an account on a self-managed Blockchain wallet and submit the public key to the healthcare authority. Subsequently, Healthcare authority confirms the eligibility of the Healthcare provider and registers the Blockchain account address, medical ID and name of the Healthcare provider on the Blockchain. The Healthcare provider can henceforward issue COVID-19 certificates. Equivalently, the service provider must acquire the authorization from a local authority after submitting his/her Blockchain account address, service ID and his/her name to become an authorized Verifier.
2. *User's logging to NovidChain*
   Prior to the COVID-19 test/vaccine certificate issuing, the healthcare provider checks the user's official physical ID (i.e., passport/ card ID) and scans the QR code of the user's Blockchain account address to interact with user identity

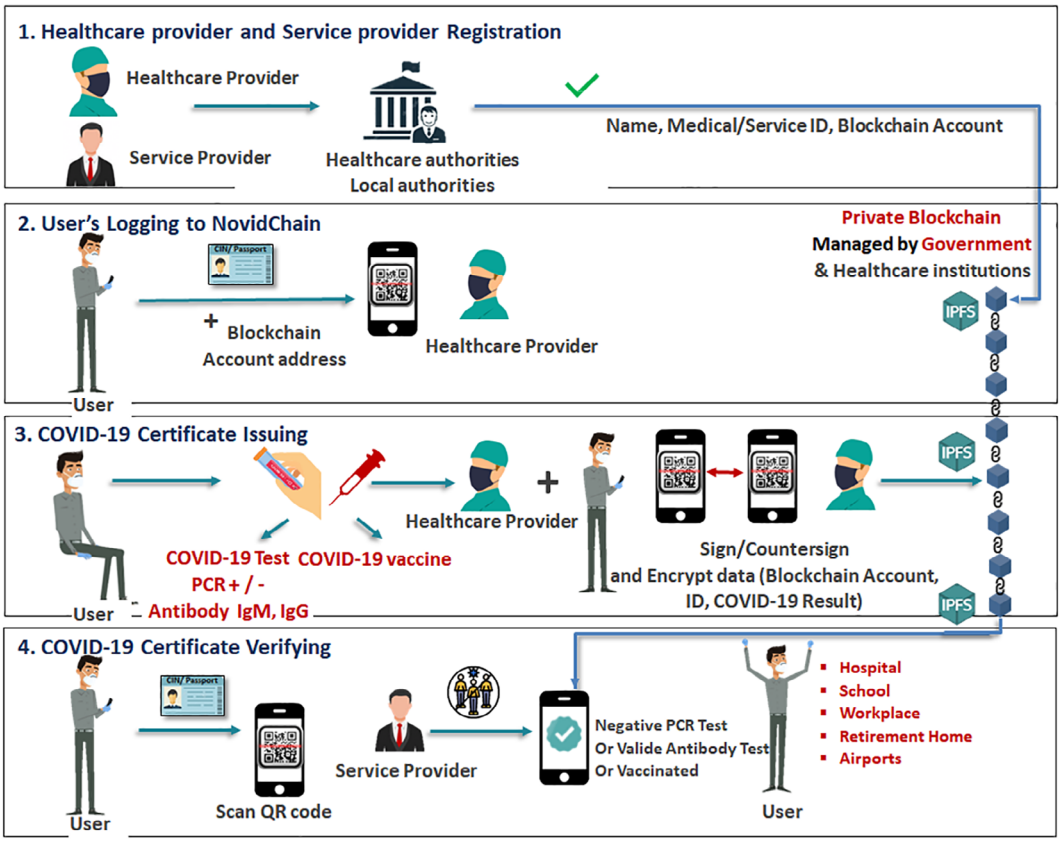


FIGURE 5 NovidChain approach overview [Colour figure can be viewed at wileyonlinelibrary.com]

for the first time. Otherwise, the healthcare provider checks if the user already has a valid certificate, since a user can have at most one valid certificate associated with him/her at any time. Note that the user must install a self-managed Blockchain wallet and create a Blockchain account before visiting the healthcare provider.

3. *COVID-19 certificate issuing*

   The Healthcare provider carries out PCR or Antibody test, or COVID-19 vaccine for the user. At that time, he/she registers user personal details, Blockchain account address, corresponding test result, and validity date in the off-chain storage after signing and encrypting these data. Meanwhile the hash of these encrypted data is stored in the Blockchain. Finally, the user acquires a digitally-signed and counter-signed COVID-19 test/vaccine certificate and is able to present a provably valid COVID-19 certificate to the Service provider. In the case of a person being re-infected or the test being false, his/her certificate can be updated by the Healthcare provider. Furthermore, if the validity period of the certificate is expired, this operation can be done automatically.

4. *COVID-19 certificate verifying*

   Proofing an individual's COVID-19 health status can be fulfilled by presenting the QR code and the official physical ID utilized in the registration step. Hence, at the entrance of public spaces, the Service provider can check the user's COVID-19 certificate by scanning the QR code. Meanwhile, the COVID-19 health status and the physical ID number are displayed. The Service provider compares the physical ID number on the COVID-19 certificate with the displayed ID number and compares also the hash stored in the Blockchain by the hash of the encrypted signed data presented as QR code. Finally, the Service provider enables/disables users' entrance to the public space.

4 | DECENTRALIZED IDS, VERIFIABLE CREDENTIALS, AND SELF-SOVEREIGNTY IN NOVIDCHAIN

This section provides more details about NovidChain approach and illustrates how NovidChain ensures self-sovereign identity (SSI) and GDPR and KYC privacy requirements while relying on open standards.

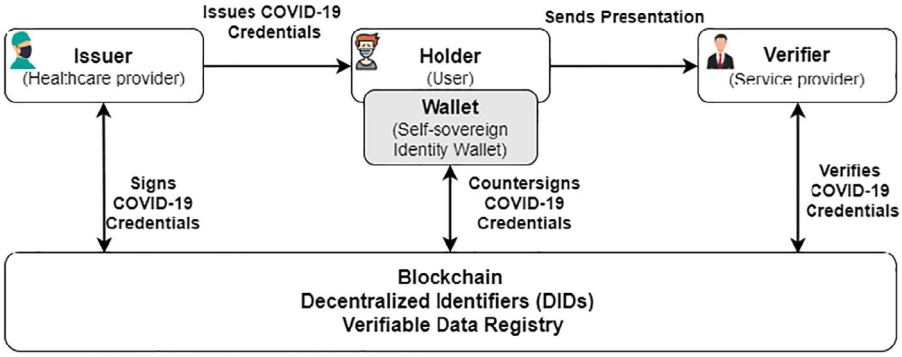


FIGURE 6 NovidChain verifiable credential model [Colour figure can be viewed at wileyonlinelibrary.com]

NovidChain is a Blockchain-based solution for secure COVID-19 credentials, in which users are allowed to generate cryptographic proofs to prove selective pieces of information about the underlying identity. Therefore, in order to protect personally identifiable information, NovidChain should be based on a self-sovereign decentralized identity system over Ethereum Blockchain.

In traditional cryptographic identity systems, public keys serve as identities. Identity ownership is acquired by possession of the private key that controls the public key. This public/private key model has many beneficial properties that have been utilized in cryptographic identity systems for years without much needed infrastructure. However, this traditional model presents some problems such as identity loss if the private keys are lost/thefted and difficulty of key revocation without extra centralized infrastructure.

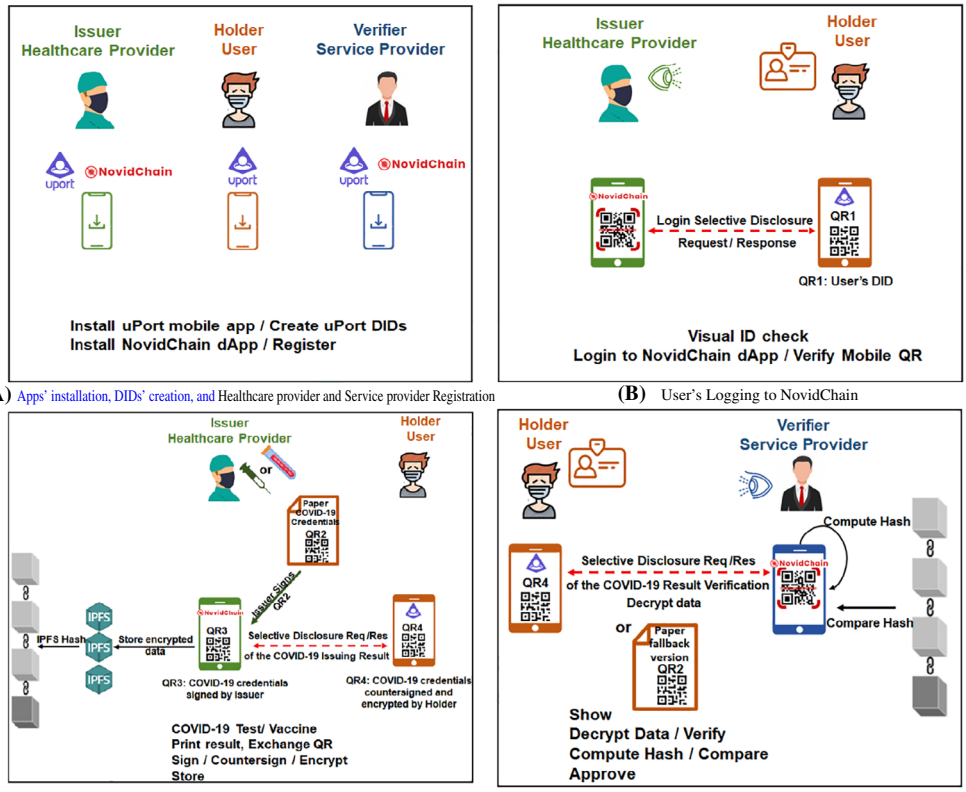
Therefore, we have chosen to rely on a new generation of digital identities known as decentralized IDs (DIDs), which present a standard for creating unique identifiers for users. More precisely, DIDs allow a self-sovereign user-centric identity, hence users are the owner of their identity and have complete control over personal data and issued digital credentials. These latter can be self-custodied and shared only with chosen trusted parties. More precisely, NovidChain relies on uPort,[23] an ethereum-based self-sovereign identity platform, in which identities are represented by DIDs that are always created by the users themselves. The most important NovidChain DIDs' feature is ensuring various privacy requirements such as GDPR and KYC. Indeed, NovidChain is GDPR-Compliant since it relies on solid common standards for data protection such as W3C VC, ERC1056 Lightweight Ethereum Identity and JSON Web Tokens (JWT), and users can be sure that they are in control of their personal information. Besides, NovidChain is KYC-Compliant since it verifies the identity of different users before onboarding them. This would allow more secure interactions and control over the data that accumulates around a specific identity and would help in collecting true information about the population's state of immunity in our case.

Figure 6 illustrates the VC role model which includes an Issuer, a User, and a Verifier. In addition, the proposed Verifiable Data Registry is an Ethereum private Blockchain. For example, a healthcare provider (Issuer) issues COVID-19 credentials to a user (Holder), who then presents it to a service provider or his/her employer (Verifier), when accessing the workplace. Besides, Figure 6 depicts the specific case of storing DIDs, and using them for signing, countersigning and verifying COVID-19 credentials. Every DID has a linked public-private key pair which facilitates issuing and signing COVID-19 credentials. As long as the Verifier has the DID of the Issuer (typically stored within the credential itself), it is easy to look up the Issuer's public key on the Blockchain and verify the signature on the credentials. Such a look-up does not involve any transactions, and thus incurs neither delay nor payment.

5 | NOVIDCHAIN IN ACTION

This section presents a detailed explanation of the design of NovidChain approach. First, we introduce different setups including DIDs' creation and the registration of the Healthcare provider and the Service provider. Then, we present the first contact of the user with NovidChain dApp through a login selective disclosure request/response. Subsequently, we explain COVID-19 credentials issuing while presenting some cryptographic mechanisms that ensure privacy. Finally, we illustrate COVID-19 credentials verifying which is ensured through Blockchain properties such as integrity and immutability.

Figure 7 depicts how NovidChain approach works to better understand its functionalities.



(A) Apps' installation, DIDs' creation, and Healthcare provider and Service provider Registration **(B)** User's Logging to NovidChain

(C) COVID-19 credentials issuing **(D)** COVID-19 credentials verifying

FIGURE 7 NovidChain in action [Colour figure can be viewed at wileyonlinelibrary.com]

5.1 | Apps' installation, DIDs' creation, and healthcare provider and service provider registration

Figure 7(A) presents different NovidChain setups including DIDs creation and registration of the Healthcare provider and the Service provider. Prior to the COVID-19 test/vaccine and certificate issue steps, we assume that all actors have the uPort and NovidChain mobile apps installed as follows:

- Both Issuer/Healthcare provider and Verifier/Service provider install the self-sovereign identity Wallet, uPort app, and submit the uPort DID and personal details to the authority. Then, the authority confirms the eligibility of the Issuer or Verifier and registers the uPort DID, medical/service ID, and other personal details on the Blockchain.
- Issuer/Healthcare provider installs NovidChain dApp and login with his/her uPort DID which allows him/her to acquire the "Issuer" role. The same thing is applied to Verifier/Service Provider who acquires the role "Verifier."
- Holder/User also installs uPort app from the Apple/Google Store and creates an account. uPort Identity creation is as easy as creating a regular key pair Ethereum account, which means that it is free of gas costs and all Ethereum accounts are valid identities. Moreover, uPort allows identities to be represented as an object that can fulfill actions such as updating its DID-document, signing messages, and verifying messages from other DIDs. More specifically, it allows the user to recover access to his/her identity in case of phone loss. With this setup, the User is in complete control of his/her identity and all his/her associated data and cannot lose access due to private key loss. Note that, as the ERC-1056 standard is used, a user needs to create only an Ethereum key pair without the need to neither generate smart contracts for key management, nor execute a transaction. Therefore, the identity creation process is so fast and seamless that millions of identities could be created in a single day,[25] ensuring good concordance with a governmental identity project.

5.2 | User's logging to NovidChain

Figure 7(B) depicts the first contact of the user with NovidChain dApp through a login selective disclosure request/response. Here, the Holder/User has created his/her uPort DID and may now visit the healthcare provider to perform the

COVID-19 test/vaccine and register himself/herself in NovidChain platform. To do so, the healthcare provider checks the user's official physical ID (i.e., passport/card ID) and scans the QR code of uPort DID, "QR1," to interact with user identity for the first time. Otherwise, the healthcare provider checks if the user already has a valid certificate, since a user can have at most one valid certificate associated with him/her at any time. Afterward, the Holder/User must login to NovidChain. Here, the user's uPort DID and personal data (e.g., physical ID number) are requested and the user can allow or deny this request from the uPort mobile app. This is called a selective disclosure request. It represents the primary means by which to validate the credentials of a Holder/User, and hence gives him/her complete control over their personal data. Once the login is done successfully, the healthcare provider can perform PCR or Antibody test, or COVID-19 vaccine.

5.3 | COVID-19 credentials issuing

Figure 7(C) clarifies COVID-19 credentials issuing, in which the Issuer/Healthcare provider carries out the COVID-19 test or vaccine. In case of COVID-19 test, the result is available within approximately 15 minutes for Antibody test and 48 hours for PCR test. Here, a positive outcome corresponds to the presence of antibodies above an appropriate threshold or the absence of the virus. Once the result is available, the Issuer/Healthcare provider issues a paper version of the COVID-19 credentials. Then, the issuer scans the printout QR code, "QR 2," with NovidChain dApp to generate a digitally-signed test result as a new QR code, "QR 3." This QR code, "QR 3," is transmitted to Holder/User, who in turn scans this new QR code with uPort app and digitally countersigns it as approval of receipt, creating thus Holder/User's own "QR 4." To explain in more detail, this data transmission is done through a selective disclosure request which can be confirmed or denied by the user. Meanwhile, the Holder/User encrypts the COVID-19 credentials and their associated signatures. The Holder/User also signs the request with the private key on his/her device and sends over the result. Once the selective disclosure response is acquired by the Issuer/Healthcare provider, this latter stores encrypted personal data including COVID-19 credentials in a secure off-chain IPFS storage. Only the IPFS hash (i.e., SHA-256 hash of the data), which is acting as a data pointer, is stored on-chain, allowing sensitive information to never be revealed to others scanning the Blockchain. Finally the hash of the stored encrypted data represents actually the QR code, "QR 4," owned by the Holder/User.

Note that, QR code "QR 2," which is not digitally signed, can be used as a rescue or fallback version in case of mobile phone loss or certain preference of the Holder or Verifier, notably during early familiarization with the digital certificate.

5.4 | COVID-19 credentials verifying

Figure 7(D) illustrates COVID-19 credentials verifying. At this step, the Holder/User has the signed and counter-signed COVID-19 test/vaccine credentials (QR 4) and a rescue/ fallback certificate (QR 2), and is able to present a provably valid COVID-19 certificate to the Verifier/Service Provider. The Holder/User must present not only the COVID-19 certificate, but also some proof of identity in order to avoid someone else impersonating him/her. Therefore, the Holder/User must display, at verification time, the same official physical ID used in the registration step. When the Verifier/Service Provider wants to verify COVID-19 credentials, he/she must decrypt the Holder/User data. This allows him/her to verify both signatures (Issuer and Holder), uPort DID, the COVID-19 result, and physical ID number. To decrypt Holder/User data, uPort uses the Box Public Key Authenticated Encryption Algorithm[26] and proposes an ERC-1098 cross-client method[27] for requesting encryption/decryption which enable a whole new wave of decentralized applications that would allow users to securely store their private data in databases. In this algorithm, Ethereum keypairs should not be used directly for encryption, instead the Holder/User should derive an encryption keypair from the account's private key for decryption and generate a random ephemeral keypair for encryption. The Verifier/Service Provider needs to know the Holder/User secretKey to decrypt data and should require user confirmation for that. Once COVID-19 credentials are verified, the Verifier/Service Provider computes the hash of the content (i.e., "QR4") and compares it to the hash stored in the Blockchain, thus ensuring data integrity and immutability. Finally, the Verifier/Service Provider can confirm the acceptance of COVID-19 credentials and safely announce the admission of the Holder/User.

We note here that the same process can be done by different Verifier entities including hospitals, testing centers, authorities, and airline agents. This would allow them not only to control the entrance to public spaces but also to have access to true information and make for example anonymized statistics. Particularly, it would facilitate the real-time monitoring of the population's health status for the government.

6 | IMPLEMENTATION

In this section, we present the implementation of the proposed Blockchain-based COVID-19 certificate platform, NovidChain. Particularly, we detail system components including smart contracts and NovidChain dApp and their implementations.

6.1 | NovidChain platform components

Figure 8 depicts the architecture of the proposed NovidChain platform which is composed of NovidChain and uPort smart contracts, NovidChain dApp, and uPort mobile app. More precisely, NovidChain platform relies on uPort tools and libraries to create and manage identities, and to request and exchange verified data between these identities. uPort dentities are compliant with the Decentralized Identifier (DID) specification. Additionally, user personal data is encrypted and stored in IPFS off-chain storage, only the hash of the encrypted data is stored on-chain in Ethereum private permissioned Blockchain for verification.

6.2 | Smart contracts

The proposed NovidChain platform consists of two types of smart contracts: NovidChain dApp smart contracts and uPort smart contracts, which are detailed as follows.

6.2.1 | NovidChain smart contracts

In the proposed approach, the registration process of the Healthcare Provider/Issuer and Service Provider/Verifier is performed on-chain in order to ensure transparency. Only the data of the User/Holder will be encrypted and stored off-chain.

To do so, two smart contracts have been developed: "IssuerRegistry" contract and "VerifierRegistry" contract. Listing 1 shows the implementation of the "IssuerRegistry" smart contract. This latter bears a lot of resemblance to the implementation of "VerifierRegistry" contract.

The main functions of these smart contracts are based on events to notify authority listeners of the actions taking place. This also alleviates the on-chain cost and harnesses the immutable logs of the Blockchain. Besides, we have developed a modifier to ensure that only the eligible Ethereum addresses are allowed to perform the functions. Indeed, modifiers are a Solidity feature that is used to make sure that certain conditions are met before proceeding to executing the function. Listing 1 (lines 13–16) illustrates how the modifier is implemented in a function. Hence, if the access is denied, the function remains unexecuted, and the Blockchain transaction treating the call is reverted.

Moreover, Listing 1 illustrates the different implemented functions.

- *approve*: An authority can approve the registration of the issuer who gives his/her Ethereum address and medical ID (see lines 17–22).

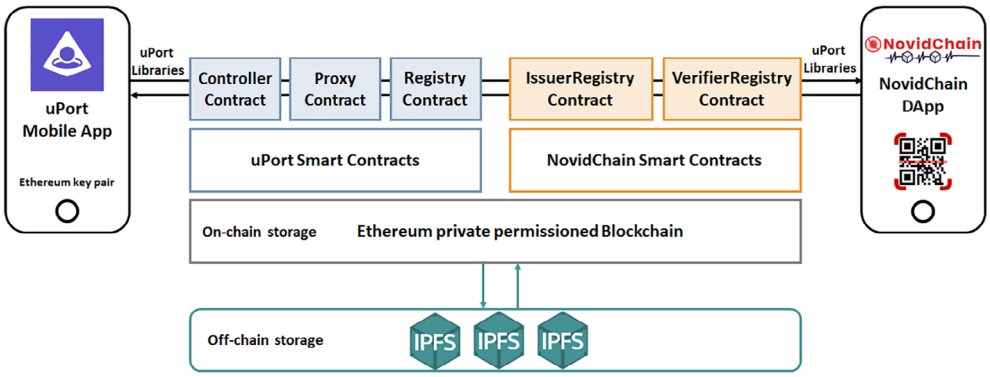


FIGURE 8 NovidChain architecture [Colour figure can be viewed at wileyonlinelibrary.com]

- *revoke*: An authority can revoke a healthcare provider from the list of authorized providers (see lines 23–28). Same functions are applied to the Service Provider in the "VerifierRegistry" contract.

```
contract IssuerRegistry {
    mapping(address=>bool) public isIssuer;
    mapping(address=>bool) public isApprovingAuthority;
    mapping(address=>bytes32) public issuerId;
    event IssuerApproved(address indexed issuer, address indexed authority);
    event IssuerRevoked(address indexed issuer, address indexed authority);

    constructor (address[] memory authorities) public {
        for (uint256 i = 0; i < authorities.length; ++i) {
            isApprovingAuthority[authorities[i]] = true;
        }
    }
    modifier onlyAuthority {
        require(isApprovingAuthority[msg.sender], "You must be an authority.");
        _;
    }
    function approve(address issuer, bytes32 id) public onlyAuthority {
        require(!isIssuer[issuer], "Already an issuer.");
        isIssuer[issuer] = true;
        issuerId[issuer] = id;
        emit IssuerApproved(issuer, msg.sender);
    }
    function revoke(address issuer) public onlyAuthority {
        require(isIssuer[issuer], "Not an issuer.");
        isIssuer[issuer] = false;
        delete issuerId[issuer];
        emit IssuerRevoked(issuer, msg.sender);
    }
}
```

Listing 1: IssuerRegistry smart contract

6.2.2 | uPort smart contracts

uPort smart contracts are available in Reference 28 and are presented as follows.

- Proxy contract: It represents the permanent identifier of a user associated with his/her private key. It allows the user to replace his/her private key without modifying his/her permanent identity.
- Controller contract: It controls the access to the proxy contract and allows the user to reclaim his/her identity in case of loss of mobile device and private key.
- Registry contract: It provides a cryptographic link between a user's uPort identifier and his/her personal data stored off-chain.

More details, about how uPort smart contracts work, are given in Section 2.3.

6.3 | NovidChain dApp

In order to allow creation and validation of identity data in NovidChain, we use uPort Credentials. This latter is a uPort library that enables the process of identity creation within NovidChain application and allows to sign and verify data to facilitate secure communication between parties. These pieces of data, referred to as credentials, take the form of signed JSON Web Tokens (JWTs) and are presented as QR code. Additionally, uPort Transports library is used to pass credentials between NovidChain application and the user via the uPort mobile app.

Five underlying implementations were performed:

1. Obtaining NovidChain dApp identity;
2. Login to NovidChain dApp;
3. Creating and issuing COVID-19 credentials;
4. Requesting and verifying COVID-19 credentials;
5. Encrypting/Decrypting the request.

6.3.1 | Obtaining NovidChain dApp identity

The first order of business to create NovidChain server side with uport-credentials is to acquire an application identity. This identity is used to sign requests, since it is considered as an Ethereum key pair with a few extra capabilities made possible by adhering to ERC-1056.

Listing 2 shows the output from the identity creation of NovidChain dApp. Note that the private key should be kept secure, it is shown here for information purposes only.

```
const { Credentials } = require('uport-credentials');
Credentials.createIdentity();
Output:
{
  did: 'did:ethr:0xc712b4034eE0e1d0AbEE50b179aD57A882bCB1Fb',
  privateKey: '5e298fa482f4f07000c680170721993f9a9bfe99e34432279bd8712e2dcd050c'
}
```

Listing 2: Obtaining NovidChain dApp identity

6.3.2 | Login to NovidChain dApp

In this subsection, we detail the implementation of the login to NovidChain dApp which requests verified data about the user ethereum identity. More precisely, identity data is requested and a uPort client representing the ethereum identity approves the disclosure of the requested information. This is called a selective disclosure request and is the primary means by which to validate the credentials of a user. After NovidChain server-side business logic has been satisfied with the disclosed data, a user can be considered authenticated through the verified credentials he/she disclosed.

The NovidChain server-side login service that uses uPort for authentication involves:

- The creation of a disclosure request message as a JWT to be consumed by the mobile application presented as QR code;
- A callback server to post selective disclosure responses back to.

Listing 3 shows the implementation of Login Selective Disclosure Request. Here, the endpoint listens for an incoming login request (lines 1–4) and generates a message encoded as a JWT formed into a URL (line 7). A QR code will be generated from the JWT URL using the uPort-Transports utility function, and displayed when the endpoint is requested (lines 8-9). The contents of the login request include mobile user's full name, physical ID number, and permission to push notifications.

```
1  credentials.createDisclosureRequest({
2    requested: ["fullName", "physicalID"],
3    notifications: true,
4    callbackUrl: endpoint + '/callback'
5  }).then(requestToken => {
6    console.log(decodeJWT(requestToken))  //log request token to console
7    const uri = message.paramsToQueryString(message.messageToURI(requestToken), {
8    callback_type: 'post'})
9    const qr =  transports.ui.getImageDataURI(uri)
10   res.send(`<div><img src=$"{qr}"/></div>`)
11 })
```

Listing 3: Disclosure Request Login Service

Listing 4 shows the Disclosure response of the authentication service. On each request, the response will be sent to a callback URL that is defined when the request is made. A second endpoint to capture that response is necessary. This callback endpoint will feed the response token from the disclosure request to a function *authenticateDisclosureResponse()* which will verify the signature of the response payload and the signatures of credentials included in the response (lines 3–7). It is at this point that proprietary authorization logic can be applied.

```
1  const jwt = req.body.access_{t}oken
2  console.log(jwt);
3  credentials.authenticateDisclosureResponse(jwt).then(credentials => {
4    console.log(credentials);
5    // Validate the information and apply authorization logic
6  }).catch( err => {
7    console.log(err)
8  })
```

Listing 4: Disclosure Response Authentication Service

6.3.3 | Creating and issuing COVID-19 credentials

In this subsection, we detail the implementation of creating and issuing COVID-19 credentials from NovidChain dApp using uPort Credentials. This task should be performed by an authorized healthcare provider.

Attesting information about users will enable them to build up their digital identity and add real value to NovidChain dApp. Additionally, this allows them to have a frictionless "proof of being a human" verification across the decentralized web. More precisely, by presenting a credential to a user, NovidChain dApp is cryptographically signing a claim about that user, and as a result, attesting to the truth of a piece of information about them. Anyone who has access to NovidChain application's DID can then confirm that a specific credential for an identity came from NovidChain dApp. For example, in our case, NovidChain dApp requests and verifies a user's full name and physical ID number during on-boarding, then that user can receive COVID-19 result credential.

At a high level, issuing a credential involves:

- Cryptographically signing user data on behalf of NovidChain application;
- Send credentials as a JWT to users via a QR code or push notification.

Listing 5 shows the implementation of Selective Disclosure Request of the COVID-19 issuing result. To do so, we provide an endpoint to ask for credentials from the user and request permissions for pushing notifications. Here, the Credentials object creates messages containing COVID-19 verified data by calling the *createDisclosureRequest()* method (lines 1–5). The disclosure request is a JWT, signed by NovidChain dApp identity that requests specific information from the user. More specifically, we request the ability to send push notifications to the user by including the notifications: "true" for "key-value pair" (line 2). When the user receives a request on his/her mobile app, he/she is asked to approve the disclosure of the requested COVID-19 attributes and their Decentralized Identifier (DID).

```
1  credentials.createDisclosureRequest({
2    notifications: true,
3    callbackUrl: endpoint + '/callback'
4  }).then(requestToken => {
5    console.log(decodeJWT(requestToken))  //log request token to console
6    const uri = message.paramsToQueryString(message.messageToURI(requestToken), {
7    callback_{t}ype: 'post'})
8    const qr =  transports.ui.getImageDataURI(uri)
9    res.send(`<div><img src="${qr}"/></div>`)
10 })
```

Listing 5: Selective Disclosure Request of the COVID-19 issuing result

Once the user scans the QR code with his/her mobile app, he/she will receive an alert about to share his/her information. Afterward, when the user verifies and accepts to share the COVID-19 result, a credential will be created from the information contained in the signed JWT access token that is returned in the disclosure response. Listing 6 shows the implementation of COVID-19 issuing result Selective Disclosure Response. The credential requires three fields: "sub," which identifies the subject (i.e., user) of the claim; "exp," which is the Unix epoch timestamp, in seconds, in which the claim should no longer be considered valid; and "claim," which contains the COVID-19 data being signed (see lines 5-11). This COVID-19 claim is a serializable JavaScript object in JSON format.

```
1  const jwt = req.body.access_token
2  credentials.authenticateDisclosureResponse(jwt).then(creds => {
3    // take this time to perform custom authorization steps... then, set up a push transport
4      with the provided push token and public encryption key (boxPub)
5    const push = transports.push.send(creds.pushToken, creds.boxPub)
6    credentials.createVerification({
7      sub: creds.did,
8      exp: Math.floor(new Date().getTime() / 1000) + 90 * 24 * 60 * 60, //90 days
9      claim: {'Identity' : {'Covid-19 Result' : `${getCovidResult()}`}}
10     // Note, the above is a complex (nested) claim.
11     // Also supported are simple claims:  claim: {'Key' : 'Value'}
12   }).then(attestation => {
13     console.log(`Encoded JWT sent to user: ${attestation}`)
14     console.log(`Decodeded JWT sent to user: ${JSON.stringify(decodeJWT(attestation))}`)
15     return push(attestation)  // *push* the notification to the user's uPort mobile app.
16   }).then(res => {
17     console.log(res)
18     console.log('Push notification sent and should be recieved any moment...')
19     console.log('Accept the push notification in the uPort mobile application')
20     ngrok.disconnect()
21   })
22 })
```

Listing 6: Selective Disclosure Response of the COVID-19 issuing result

Listing 7 shows the output of the createVerification() function which returns a promise that resolves to a JWT. A push notification will appear in the mobile app of the user who has just scanned the QR code, containing the credential depicted in Listing 7.

```
{
  "header": {
    "typ": "JWT",
    "alg": "ES256K-R"
  },
  "payload": {
    "iat": 5765731856,
    "sub": "did:ethr:0xd1422f53e3b7bccc4a7ddd9a0123b67f659e8211",
    "claim": {
      "Covid-19 Result": {
        "Last Seen": "Fri Dec 25 2020 07:25:01 GMT+1"
      }
    },-
    "exp": 5765731856,
    "iss": "did:ethr:0xc712b4034eE0e1d0AbEE50b179aD57A882bCB1Fb"
  },
  "signature": "Am5_{0}Bc-5YrEeHOVSCQbukYfFRphJqL07IEWZb7RvH7S7_{E}FE8YsdsV31c58qyS8jO-
  ML24ursVl_{d}Z4ikQST7A",
  "data": "cyK0eXAiOiJKG1OiLCJhbGciOiJFUzI1NkstUiJ3.
  eyJpYXQiOjE1NCExMzc4MzQsInN1YiI6ImRpZDpldGh.yOjB4Y2YzMTFlNTNlM2I3YjI3YzRhN2NjZDlhMGYzMW.
  I2OGY2NTllODI5MSIsImNsYWltIjp7IkQ4YW1wbGUiO.nsiTGFzdDBBZWVuIjoiRnJpIE5vdiAwMiAyMDE4IDTx.
  OjUwOjN0IEdNVC0wNDAwICHFRFQpIn19LCJleHAiOjE.1NDM3Mjk4MzQsImlzcyI6ImRpZDpleGhyOjA3MzE0OD.
  KwNTRhNlFkMmMwYjY4NWNyODljZTBiATAxOGUyMTCkNTA0ZSF5"
}
```

Listing 7: COVID-19 credentials

6.3.4 | Requesting COVID-19 credentials

In this subsection, we detail the implementation of requesting COVID-19 credentials from NovidChain dApp using uPort Credentials. This task should be performed by an authorized service provider.

Requesting COVID-19 credentials is the same process as creating a disclosure request as seen before.

At a high level, requesting a verification involves:

- Cryptographically sign a request to disclose user data on behalf of NovidChain dApp.
- Send a request as a JWT to the user via a QR code or push notification.

Listing 8 shows the implementation of the COVID-19 credentials request. Here, we provide an endpoint to ask for COVID-19 verified credentials from the user (lines 1–4). In this situation we are including a request for a verified claim with the verified array, and the user will be prompted to approve the requested credentials (lines 7-8).

```
1  credentials.createDisclosureRequest({
2    verified: ['Covid-19 Result'],
3    callbackUrl: endpoint + '/callback'
4  }).then(requestToken => {
5    console.log(decodeJWT(requestToken))  //log request token to console
6    const uri = message.paramsToQueryString(message.messageToURI(requestToken), {
7    callback_{t}ype: 'post'})
8    const qr =  transports.ui.getImageDataURI(uri)
9    res.send(`<div><img src="${qr}"/></div>`)
10 })
```

Listing 8: COVID-19 credentials verifying request

Once the user accepts to respond to the request, a verification will be created from the information contained in the signed JWT access token that is returned in the disclosure response. Listing 9 shows the implementation of the COVID-19 verification response. Afterward, when the service provider obtains the JWT, he/she should validate it. The *authenticateDisclosureResponse()* function is used to validate the JWT by checking that the signature matches the public key of the issuer (lines 2–4). This validation is done both for the overall JWT and for the JWTs that are sent in the larger payload (lines 6-7). The service provider can also verify the physical ID number from this payload.

```
1  const jwt = req.body.access_token
2  console.log(jwt)
3  console.log(decodeJWT(jwt))
4  credentials.authenticateDisclosureResponse(jwt).then(creds => {
5    //validate specific data per use case
6    console.log(creds)
7    console.log(creds.verified[0])
8  }).catch( err => {
9    console.log("error")
10 })
```

Listing 9: COVID-19 credentials verifying response

6.3.5 | Encrypting/decrypting the request

uPort uses the ERC 1098 encryption method[27] which uses an ephemeral sending key and the box method from tweet-nacl.[29] This allows the Verifier/Service Provider to decrypt a message without having to resolve the public key of the Holder/User.

The following encryption method should be used by the Holder/User:

1. Create the signed JWT payload like normal;
2. JWT is padded with \0s to the nearest multiple of 64 bytes;

3. Create an ephemeral keypair using nacl.box.keyPair();
4. Create a random 24 bytes nonce using nacl.randomBytes(nacl.box.nonceLength);
5. Encrypt the resulting JWT using the nacl.box(message, nonce, recipient publicKey, ephemeralKeyPair.secretKey);
6. Combine the base64 encoded versions of the nonce, ephemPublicKey and ciphertext values together with the version of x25519-xsalsa20-poly1305 in a JSON payload.

To decrypt the request, the Verifier/Service Provider needs to know the Holder/User's secretKey and should use the following method.

1. Check that the version field is x25519-xsalsa20-poly1305;
2. Decode the base64 encoded nonce, ephemPublicKey and ciphertext attributes;
3. Decrypt it message using nacl.box.open(ciphertext, nonce, ephemPublicKey, recieverEncryptionPrivateKey);
4. Strip any trailing \0 from the payload;
5. Decode JWT as normal;

7 | EXPERIMENTS

This section illustrates several experiments to validate the feasibility and performance of the NovidChain platform. Note that the the source code of NovidChain dApp is available on Github in Reference 30.

As mentioned before, the main component of NovidChain platform is NovidChain dApp which interacts with the uPort Mobile App to ensure self-sovereign identity management for COVID-19 certificates.

Based on this developed NovidChain dApp, three underlying operations were performed:

- Login/connecting to NovidChain dApp with uPort Mobile App;
- Creating and issuing COVID-19 credentials;
- Requesting and verifying COVID-19 credentials.

To start with the login operation, NovidChain dApp generates a QR code which is scanned by the uPort Mobile App, and hence establishing the first interaction as shown in Figure 9. Once NovidChain dApp is connected with uPort Mobile App, NovidChain dApp issues a COVID-19 credential and sends it to uPort Mobile App. When the credential is accepted by the holder, it is stored in his/her digital wallet on the mobile device as shown in Figure 10. NovidChain dApp is utilized for both objectives creating and issuing COVID-19 credential, and requesting and verifying COVID-19 credentials. Hence, thanks to NovidChain dApp, the credential can be transmitted to the verifier for its verification to benefit from his/her services, which is illustrated in Figure 11. In summation, the three mentioned

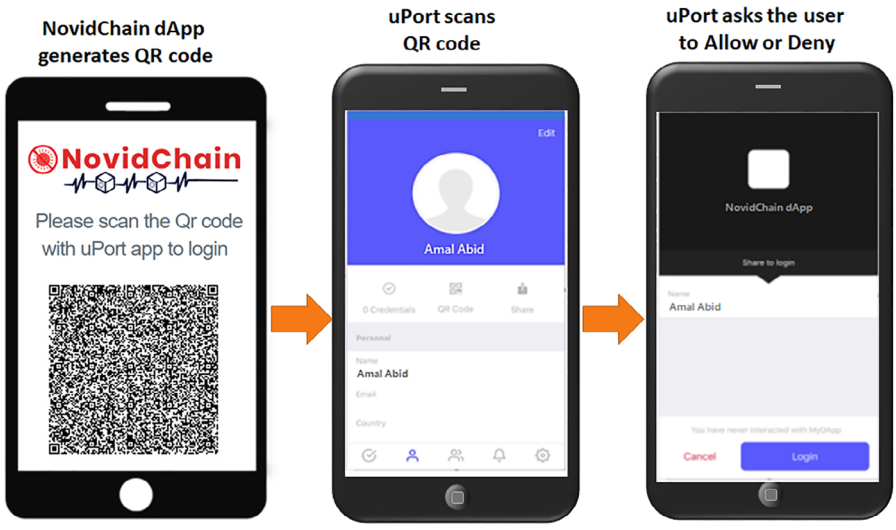


FIGURE 9 Validation: Login to NovidChain dApp [Colour figure can be viewed at wileyonlinelibrary.com]

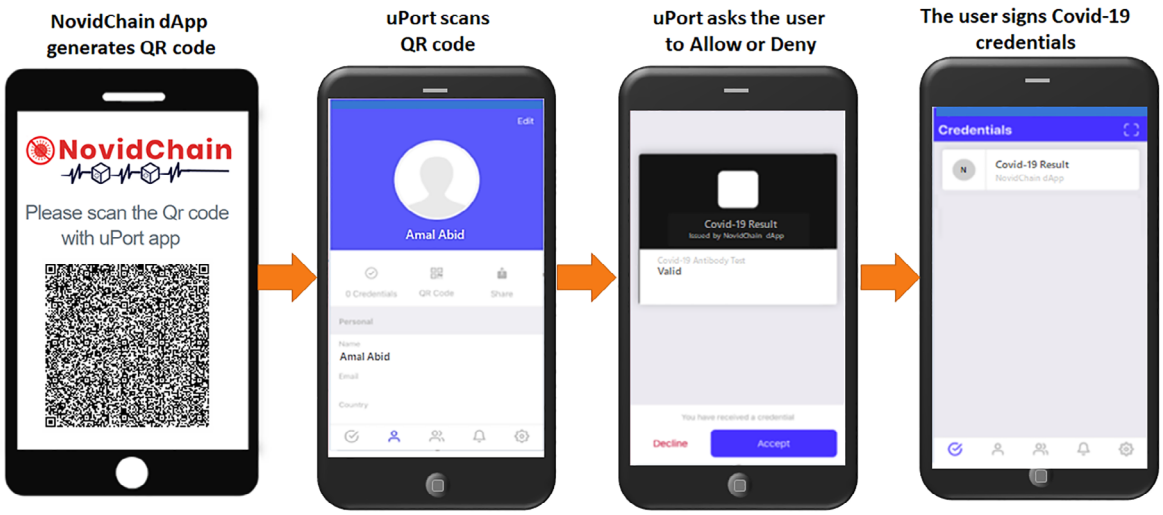


FIGURE 10 Validation: Creating and issuing COVID-19 credentials [Colour figure can be viewed at wileyonlinelibrary.com]

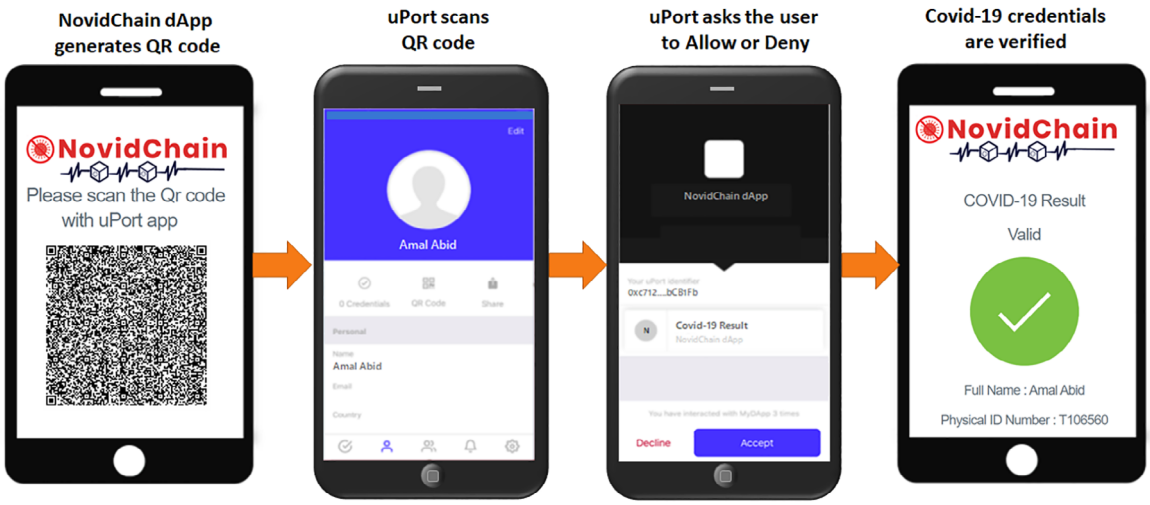


FIGURE 11 Validation: Requesting and verifying COVID-19 credentials [Colour figure can be viewed at wileyonlinelibrary.com]

identity management operations were carried out using NovidChain dApp to consider and explore the obtained results based on experiments.

8 | EVALUATION

This section evaluates the proposed NovidChain platform and shows its security and efficiency for use within real-world settings including security properties, financial cost, and scalability. This evaluation is made by comparing NovidChain with two academic work and one commercial work, namely SecureABC,[31] CATCApp,[32] and ImmuPass,[13] respectively. The selection of these work was basically decided on practical grounds, as they have presented a detailed specification for their implementations. More precisely, both CATCApp and ImmuPass are based on Blockchain technology except that the first uses an off-chain storage while the second uses an on-chain storage. SecureABC, on its part, relies only on basic cryptographic primitives and does not use Blockchain. These three solutions will be taken into consideration in the following evaluation.

The comparison of NovidChain with CATCApp, SecureABC, and ImmuPass is presented in Table 1. Evaluation results are discussed afterward.

TABLE 1 Comparative evaluation of COVID-19 certificate solutions

		Security properties						
Approach	**Type**	**Forge**	**Binding**	**Uniqueness**	**Peer-Indistinguishability**	**Revocation**	**Low cost**	**Scalability**
SecureABC	Crypto-graphy	+/-	-	+	+	+/-	not available	not available
CATCApp	Blockchain-based	+	+	+	-	-	+	-
ImmuPass	Blockchain-based	+	+	+	-	+/-	-	-
NovidChain	Blockchain-based	+	+	+	+	+	+	++/-

8.1 | Security properties

We consider the following security properties: forge/tamper proof, binding, uniqueness, peer-indistinguishability, and revocation.

- *Forge and tamper proof*
  Forge and tamper proof properties are satisfied if a user cannot create a valid certificate alone, or alter a value of the attributes associated with a certificate. For NovidChain, we require that the Ethereum signature scheme is Strong Existential Unforgeability under Chosen Message Attack (SUF-CMA) secure therefore no forgery of the signature on certificates is possible. Moreover, in order to tamper with the certificate value, an adversarial user must also forge the corresponding signature in all Ethereum Blockchain nodes at the same time, which adds a second level of security. This property is also satisfied by CATCApp and ImmuPass, but less satisfied by SecureABC, which is only Existential Unforgeability under Chosen Message Attack (EUF-CMA) secure.
- *Binding*
  Binding property is satisfied, if a user can successfully use only the certificate that is assigned to him/her and which has not been revoked. This prevents a user from using a certificate that was not issued to him/her. In NovidChain, a tested user is bound to his/her certificate by the official document ID (passport/ID) that is signed by a healthcare provider. This can be considered as a strong binding property. In addition, it is in line with current socially accepted verification mechanisms. This property is also satisfied for CATCApp and ImmuPass which use a driving license or passport for the identification. However, SecureABC has a weak binding property as it uses a photograph for the identification which can be imperfect when considering twins or people who share similarities in their skin type and/or facial features and may look somewhat similar in photographs. Besides, wearing masks during COVID-19 pandemic could complicate identification by photograph.
- *Uniqueness*
  Uniqueness is satisfied if a user can have at most one valid certificate associated with him/her at any time. In the certificate issuing phase, the healthcare provider checks if the tested person currently has a valid certificate. Consequently, uniqueness is satisfied to the degree that it is already assured for healthcare record keeping. All proposed solutions satisfy this property.
- *Peer-indistinguishability*
  Peer-indistinguishability is satisfied if a malicious peer, defined as an unauthorized service provider/Verifier, cannot learn any information about the user while viewing the certificate. Intuitively, peer-indistinguishability ensures that a user cannot be tricked while revealing him/her certificate by anyone except an authorized service provider. The service provider/ Verifier is required to present a valid public key, signed by the government, which has not been revoked. Hence, peer-indistinguishability can be reduced to the difficulty of forging a government signature in all Blockchain nodes. Unlike, CATCApp, ImmuPass and SecureABC, this property is satisfied for NovidChain. Meanwhile, in CATCApp and ImmuPass, anyone willing to act as a Verifier can download the app and start verifying. According to CATCApp authors, there is no need to create an account for verifying a user's certificate, since Verifier does not submit data, which would harm the peer-indistinguishability properties. For SecureABC approach, only app-based authentication sub-protocol realizes the peer indistinguishability property. This is achieved by enforcing mutual authentication between a user and a verifier which cannot be performed by their paper-based approach.
- *Revocation of certificates and service providers*

We require that a user's certificate can be revoked by the healthcare provider. Certificates may be invalidated for a number of reasons, we give three examples below:

- Loss: If a certificate is lost.
- Error: If a batch of tests are recalled because they were incorrect.
- Misuse: If evidence of certificate misuse is presented.

We require that a service provider can be revoked from the list of authorized providers. An authorized service provider may be revoked in the following situations:

- Change of policy: A change in government policy may mean some service providers are no longer authorized.
- Sanctioning: If a service provider is deemed to not be following recommended guidelines it may lose its authorized status.

NovidChain and app-based version of SeureABC consider these revocations, while ImmuPass assures only the certificate revocation. CATCApp does not take these revocations into account.

8.2 | Financial cost

In Ethereum Blockchain, a transaction fee is required to perform a task (e.g., executing an ABI, storing data, etc.), which is measured by a unit called gas. The notion of gas was introduced in Ethereum for the need to protect the network from attacks.

Hence, storing data directly on Ethereum Blockchain suffers not only from confidentiality issues but also from being costly.

Giving an example of storing a user's COVID-19 credentials on-chain, which measures approximately 1 kilobyte in size. According to Ethereum's Yellow Paper,[16] a 256-bit word costs 20,000 gas. Since 8 bits sum up to one byte, so 1 word is 32 bytes. As, 1,024 bytes form 1 kilobytes, the amount of gas paid to store 1 kilobyte is equal to $32 \times 20,000\ gas = 640,000\ gas$.

The gas price in ETH is not fixed, since users select their own. According to ETH Gas Station,[33] the cheapest price as of December 2020 is 122 Gwei, or 0,000000122 ETH. Hence, to store just 1 kilobyte of data would cost $640,000\ gas \times 0,000000122 ETH = 0.078$, or \$57 at the current ETH/USD price. This means that a user should pay \$57 to store COVID-19 credentials on-chain. This amount is only for 1 kilobyte of data (i.e., an initial user's json file). To store 1 megabyte of data that includes scanned image (e.g., user's photograph, official ID document, COVID-19 X-Ray, etc.), a user should pay $57 \times 1024 = \$58,368$, which is very costly.

Therefore, in NovidChain platform, only generated IPFS hash of user data is stored in the Ethereum Blockchain, the data itself is stored off-chain.

Table 2 compares the gas cost of NovidChain with that of CACT'App and ImmuPass. Here, we focus specifically on COVID-19 certificate issuing operation, since it is the most frequent operation in these platforms. Moreover, reading/accessing data from the Blockchain to verify the hash of COVID-19 credentials, is performed instantaneously and does not cost any fees. In NovidChain and CATCApp, issuing a COVID-19 certificate corresponds to only storing the hash of user data in the Blockchain which does not cost much gas. Besides, this transaction is performed by the issuer, so the user has not to pay any transaction fee. Unlike NovidChain and CATCApp, ImmuPass stores COVID-19 credentials directly on the Blockchain. We can see from the Table 2 that ImmuPass is much more expensive than the other two platforms.

8.3 | Scalability

In order to evaluate the feasibility of NovidChain platform within a real-world setting, we first analyze the scalability of NovidChain and then compare it with other proposals.

TABLE 2 Cost of issuing a COVID-19 certificate

Approach	Gas	USD
ImmuPass	131,398	\$11.89
CATCApp	24,128	\$2.18
NovidChain	24,128	\$2.18

8.3.1 | Scalability of NovidChain

This subsection illustrates the scalability of NovidChain platform while comparing COVID-19 credentials' storage on-chain and off-chain. In fact, storing data directly on Ethereum Blockchain suffers not only from confidentiality shortcomings and high cost but also from scalability issues.

Here, we test a simple COVID-19 credentials dataset to be stored on-chain. We start with a small JSON structure of 800 bytes which corresponds to 1 user. This amount of data will be incremented by a transaction overhead of 100 bytes to store the sender's address, digital signature and a few other pieces of data. Knowing that the Ethereum Blockchain network could scale to 500 transactions per second, the total data throughput would be 450 kilobytes per second (i.e., measured from $500 \times (800 + 100)$). This constitutes under 5 megabits/second of bandwidth, which is comfortably within the capacity of any modern Internet connection. Data would accumulate at a rate of around 1 terabytes for 1 billion of users which is a manageable amount of data. Note that this amount of data would be stored and synchronized on every Blockchain node.

Things become more complicated when we need to store on-chain larger pieces of information, such as scanned documents (e.g., user's photograph, official ID document, COVID-19 X-Ray, etc.). An appropriate quality of A4 scanned paper might be 500 kilobytes in size. Multiplying this by 500 transactions per second, leads to a throughput of 250 megabytes per second. This constitutes 2 gigabits/second of bandwidth, which is faster than most local networks. Moreover, all Blockchain nodes should store more than 2000 terabytes of new generated data which is not feasible.

Therefore, to address the scalability issue, NovidChain platform relies on IPFS storage to store COVID-19 credentials off-chain. It stores on-chain only the hashes of large pieces of data, instead of the data itself. Each hash acts as an identifier to its input data, with the data itself being stored off-chain on some particular nodes of the Blockchain. Meanwhile, a 500 kilobyte JPEG image can be represented on-chain by a 32-byte number (i.e., size of a hash), which leads to a reduction of over $15,000\times$ on-chain. In the same way, the cost would be reduced extremely.

Furthermore, reading and writing operations in IPFS have great performance in terms of latency and response-time, since 1MB of data could be handled in 100 ms.[34] This enhances the scalability of NovidChain platform compared to ImmuPass, which stores COVID-19 credentials on-chain.

However, although all mentioned benefits, NovidChain remains dependent on Ethereum Blockchain's latency. In fact, despite IPFS performance, and despite the reduction of data-size sent to the Blockchain, storing users' data hashes on-chain leads to some overheads. These overheads can be calculated, if we respond to the following question. As each IPFS hash corresponds to a user, how many users can be handled in each block creation (i.e., 15 seconds)?

In order to give answer to this question, let us denote the block gas limit by $G_{blockLimit}$, the gas cost of a transaction by G_{tx}, the gas cost of every non-zero byte of data of a transaction by $G_{txDatanonzero}$, the gas cost of a *SSTORE* operation which is performed once by G_{SStore}, and the IPFS hash size by *HashSize*. Table 3 lists the corresponding values of these variables (as of December 2020).

Consequently, the maximum number of users that can be handled per block creation, is calculated as follows:

$$\frac{G_{blockLimit} - G_{SStore}}{G_{tx} + (G_{txDatanonzero} \times HashSize)} = 517 \tag{1}$$

Therefore, according to Equation (1), approximately 517 users can be handled per block creation (i.e., 15 seconds), which means 124,080 users per 1 hour.

8.3.2 | Comparative evaluation of scalability

In this subsection, we compare NovidChain scalability with those of CATCApp and ImmuPass platforms. We focus specifically on COVID-19 credentials issuing and verifying since they are the most frequent transactions in these

TABLE 3 Variable values of Equation (1)

$G_{blockLimit}$	12,500,000 gas units
G_{tx}	21,000 gas units
$G_{txDatanonzero}$	68 gas units
G_{SStore}	20,000 gas units
HashSize	46 bytes

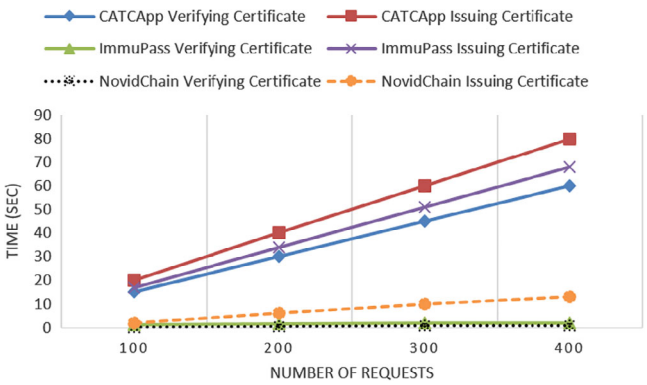


FIGURE 12 Latency evaluation [Colour figure can be viewed at wileyonlinelibrary.com]

platforms. Figure 12 exhibits the results of the experiments and the investigations, which were carried out under the same experimental condition (i.e., sending 400 simultaneous requests) so as to compare the results with CATCApp and ImmuPass.

The completion time in seconds (Y axis) of NovidChain operations where we sent between 1 and 400 simultaneous requests (X axis) is as follows. The fastest operation "Verifying COVID-19 credentials" is the lowest line, while "Issuing COVID-19 credentials" is slower than the first one. This difference in time is due to the difference between writing on the Blockchain through transactions to add an entry which is more expensive than instantaneous reading/accessing data from the Blockchain.

In addition, the experiments have been shown to decrease response-time in comparison with the approach with CATCApp. Indeed, the relative difference in time between operations implying "Issuing COVID-19 credentials" is remarkable (56%) since CATCApp performs hash generation twice (i.e., locally generated hash (LH) and server-generated hash (SH)). Moreover, we note a high and critical difference in time between operations implying "Verifying COVID-19 credentials" (49%), which are instantaneous in NovidChain since they involve only a look up at the Blockchain.

Furthermore, the relative difference in time between NovidChain and ImmuPass for "Issuing COVID-19 credentials" (46%) is obvious since ImmuPass stores data on-chain. Indeed, as mentioned before, 517 users can be handled by NovidChain in 15 seconds, while only 71 users can be handled by ImmuPass during the same duration.

Finally, linear growth for all operations confirms that NovidChain architecture is able to handle scale-up without surprise: there is simply no inter-app communication or interaction overhead.

9 | RELATED WORK

This section provides an overview of the existing COVID-19 certificate approaches and a qualitative comparison table (see Table 4).

Most of the commercial systems being trialed and implemented by governments[1-3,8,10-12,14] cannot be fully understood or reviewed since they provide few details about their approaches. Besides, most of these solutions are centralized[14] or rely on third parties,[11] thus resulting in security and privacy-preserving issues. Commercially, CoronaPass[14] proposes a centralized antibody certificate solution in which service providers verify users' passports through a central database. Although security and legal measures could be established, CoronaPass represents unavoidable risk and a central point of failure. Besides, involving the central party in each authentication leads to large scale issues. In our proposal, we rather support decentralization which is an inherent property of Blockchain. Besides, NovidChain relies on Decentralized IDs (DIDs) standard for creating unique identifiers for users through the uPort platform.

China Health code system[11] is derived from relational cross-match by scanning the QR code, which is correlated with the user. In this system, user privacy is not respected due to the fact of relying on a third party—Alipay, in which the identity of the user is not hidden. People in China sign up through Alipay wallet app, and are assigned a color code—green, yellow, or red—that reveals their health status. Besides, the system sends personal data to police, in a troubling precedent for automated social control, and is already in use nationwide. Compared to this work, NovidChain ensures the user's right to privacy while being GDPR and KYC compliant. In NovidChain, users have full control over their data and any request for accessing these data must necessarily require their confirmation.

TABLE 4 Comparison of COVID-19 certificate approaches

Approach	Infrastructure			Security features				Implementation details
	No centralization	No third party	Blockchain	Privacy-preserving	Self-sovereignty	GDPR-compliant	KYC-compliant	
CoronaPass	-	+	-	-	-	-	+	-
ChinaAlipayApp	+	-	-	-	-	-	+	-
ImmuPass	+	+	+	-	-	-	+	+
CERTUS	+	+	+	-	-	-	+	-
VaccineGuard	+	+	+	+	+	+	+	-
COVI-Pass	+	+	+	+	+	+	+	-
DigiLocker	+	+	+	+	+	+	+	-
DigitalGreen Certificate	+	+	+	+	+	+	+	-
DigitalHealthPass	+	+	+	+	+	+	+	-
CATCApp	+	-	+	-	+	-	+	+
SecureABC	+	+	-	+	+	+	-	+
NovidChain	+	+	+	+	+	+	+	+

More recently, some commercial antibody certificate solutions, relying on Blockchain technology, are proposed. The "Immupass" COVID-19 Immunity Certificate[13] stores details of the tested individual directly in a consortium Blockchain. A user obtains a QR code containing all personal information associated with the test result from the issuer. Then, when the user presents the QR code and his/her passport to a verifier, the corresponding test result and its validity is retrieved from the Blockchain. A similar approach is given by CERTUS[12] which proposes that only the hash of each user's certificate is stored in the Blockchain. Both of these works do not assume users' self-sovereignty since they act passively with the given QR code without specific control of their personnel data. Besides, storing personal data directly in the Blockchain by "Immupass" solution contradicts the GDPR privacy requirements. NovidChain differs from these works as it ensures the user's self-sovereignty. Besides, Personal Identifiable Information is anchored on the Blockchain rather than stored directly in the Blockchain.

The list of available solutions is growing day-by-day as the COVID-19 vaccine has become available. Recently, this list involves the VaccineGuard app[35] developed by Estonian authorities in collaboration with the World Health Organization, COVI-Pass[36] proposed by Tento Health company, which is considered in 15 countries including Canada and France, DigiLocker[37] developed by the government of India, Digital Green Certificate[38] introduced by the European Commission to be used across all EU countries, and Digital Health Pass[39] developed by IBM. All these solutions have proposed a Blockchain-based COVID-19 test/vaccine certificate platform. The COVID-19 test/vaccine certificate is presented as QR code indicating vaccination's details. To ensure data privacy, personal identifiable information is conserved encrypted and cannot be disclosed without the user's approval. However, most of these solutions present a high level overview of the proposed approach, with no implementation nor technical details. In particular, Blockchain details as well as users' self-sovereignty details are not available. To date (March 2021), only the Estonia VaccineGuard app is in the pilot stage, the other solutions are currently under development or in the consideration stage.[40]

A limited number of academic works taking in consideration COVID-19 certificates have been proposed, most of them were high-level sketches.[41] We think that there have been only two academic work for antibody credential systems that have presented a detailed specification for their work. First, Eisenstadt et al.[32] propose a COVID-19 antibody test certification CATCApp that combines W3C VC standard, the "Solid" platform for decentralized social applications[42] and a federated consortium Blockchain. The authors suggest that the hash of each user's certificate is stored in a consortium Blockchain which is checked afterward by verifiers at checking points. As Solid is being used for user identification and personal data control, there would be some security concerns. In fact, Solid offers no security properties or privacy properties, currently having only an access control language but no cryptographic techniques are used to encrypt data. Moreover, the core concept is that personal data can be stored locally on a device like a mobile phone or even a "favorite cloud server." It seems that giving a user the choice of where to store their COVID-19 antibody test results will likely not

lead to more security, as users may store their test results on a mobile phone whose operating system needs updating, an unsecured personal server, or in a public cloud server. It would be better to store personal data in secure enclaves. Besides, the use of RDF format has poor scalability compared to traditional relational databases or key-value stores.[43] In our proposal, we rather rely on uPort platform instead of Solid to handle all cited limits of Solid and ensure that user's data is kept private and personal.

The second interesting academic proposal SecureABC proposed by Hicks et al. in Reference 31 presents a secure Anti-Body Certificates for COVID-19. Here a cryptographically signed credential is issued to a user by the healthcare provider and can then be verified by a service provider at any time without the issuers knowledge. Although SecureABC could achieve efficient security properties yet only relying on basic cryptographic primitives (i.e., no Blockchain infrastructure), there seems to be no move toward widespread of such implementation. NovidChain differs from this work as it supports the new generation of digital identities—Decentralized IDs (DIDs)—for creating unique identifiers for users. Besides, the management of these DIDs is done efficiently through the Blockchain infrastructure.

Unlike all cited previous work, NovidChain is a Blockchain-based privacy preserving solution that ensures GDPR and KYC privacy requirements and user's self-sovereignty.

10 | DISCUSSION

Although NovidChain is capable of enhancing privacy and self-sovereignty, it can be still improved in a larger scope while considering the following aspects.

1. *Fog (Edge)/Cloud platform deployment*. In order to enhance latency, energy, network, and CPU usage of the computing infrastructure when millions of people need to be given vaccines, NovidChain can be integrated with a fog framework such as FogBus.[44] A fog framework could manage an intermediate layer between NovidChain framework and the private Cloud handled by the Government. Meanwhile, Fog nodes, which can be managed by healthcare institutions, are deployed across the edge network in a distributed manner. Through these Fog nodes, the Fog framework offers Cloud-like services such as infrastructure, platform and software closer to the user data sources and supports NovidChain execution. Therefore, it decreases service delivery time and network congestion, and enhances Quality of Service (QoS) and user experience. However, unlike Cloud datacenters, Fog nodes are resource constrained in which it is not possible to perform large scale operations. Therefore, coherent integration between Fog and Cloud infrastructure is required so that both edge and remote resources can be exploited according to dynamic requirements of NovidChain application. More appreciably, FogBus applies Blockchain, authentication, and encryption techniques to ensure data integrity, protection, and privacy. This would facilitate the integration of NovidChain into FogBus.
2. *Vaccination prioritization strategies*. Another concern, which is no less important to take into consideration, is the COVID-19 vaccine prioritization strategies. While current approaches are using combinations of age-based, chronic disease-based and occupation-based prioritizations, using multi-factor-based and social contact network-based prioritizations can enhance the distribution of the limited number of vaccine doses.[45] Furthermore, using machine learning algorithms to provide accurate and real-time prediction of the growth behavior of the epidemic while giving vaccines, is crucial for Governments. In fact, a poorly fitting model could induce a non-optimal decision-making, leading to breakdown of the public health situation.[46] Particularly for NovidChain, using these machine learning prediction algorithms could help to estimate the data-size growth and its impact on the scalability of NovidChain platform with time, and hence could help to respond proactively.

11 | CONCLUSION

In this article, we proposed NovidChain: a Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificate issuing and verifying. NovidChain facilitates instant verification of tamper-proof COVID-19 test/vaccine and thus helping to mitigate the spread of COVID-19 disease, while protecting the user's right to privacy. Indeed, NovidChain relies on a set of emerging technologies such as Blockchain, uPort Self-Sovereign Identity platform and IPFS storage to ensure privacy requirements such as GDPR and KYC. We provided a detailed technical description, a proof-of-concept implementation, different experiments, and a comparative evaluation.

In future work, we aim to enhance NovidChain platform by integrating Fog (Edge)/Cloud infrastructure and machine learning algorithms for vaccination prioritization strategies. We also plan to contribute more generally to the development of any Health Certificate solution based on the proposed approach which constitutes a first step toward privacy-preserving Digital Health Certificate solutions.

ORCID

Amal Abid https://orcid.org/0000-0003-0669-8406
Saoussen Cheikhrouhou https://orcid.org/0000-0003-4607-7452
Slim Kallel https://orcid.org/0000-0002-2824-167X
Mohamed Jmaiel https://orcid.org/0000-0002-2664-0204

REFERENCES

1. Sharma A, Bahl S, Bagha AK, Javaid M, Shukla DK, Haleem A. Blockchain technology and its applications to combat COVID-19 pandemic. *Res Biomed Eng*. 2020;1-8. https://dx.doi.org/10.1007%2Fs42600-020-00106-3.
2. Kalla A, Hewa T, Mishra RA, Ylianttila M, Liyanage M. The role of blockchain to fight against COVID-19. *IEEE Eng Manag Rev*. 2020;48(3):85-96.
3. Khurshid A. Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. *J Med Internet Res Med Inform*. 2020;8(9):e20477.
4. Bay J, Kek J, Tan A, et al. *BlueTrace: A Privacy-Preserving Protocol for Community-Driven Contact Tracing Across Borders. Technical Report*. Singapore, Asia: Government Technology Agency-Singapore; 2020.
5. The security behind the NHS contact tracing app; 2020 [Online]. https://www.ncsc.gov.uk/blog-post/security-behind-nhs-contact-tracing-app.
6. Xu H, Zhang L, Onireti O, Fang Y, Buchanan WB, Imran MA. BeepTrace: blockchain-enabled privacy-preserving contact tracing for COVID-19 pandemic and beyond; 2020. arXiv preprint arXiv:2005.10103.
7. NHS rejects apple-Google coronavirus app plan. *BBC News* [Online]. https://www.bbc.com/news/technology-52441428.
8. Phelan AL. COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges. *Lancet*. 2020;395(10237):1595-1598.
9. Estonia tests first digital immunity passports for workplaces; 2020 [Online]. https://eandt.theiet.org/content/articles/2020/05/estonia-tests-first-digital-immunity-passports-for-workplaces/.
10. Fraser B. Chile plans controversial COVID-19 certificates. *Lancet*. 2020;395(10235):1473.
11. In coronavirus fight, China gives citizens a color code, with red flags; 2020 [Online]. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.
12. Sicpa CERTUS - A COVID-19 health passport secured by blockchain to enable deconfinement; 2020 [Online]. https://www.sicpa.com/news/covid-19-health-passport-secured-blockchain-enable-deconfinement.
13. ImmuPass A simple and secure certificate of COVID-19 immunity; 2020 [Online]. https://www.immupass.org/.
14. CoronaPass-FAQ. Bizagi; 2020 [Online]. https://resourcesbizagi.azureedge.net/docs/coronapass/CoronaPass-FAQ.pdf.
15. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Cryptography mailing list; 2008.
16. Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*. 2014;151:1-32.
17. Abid A, Cheikhrouhou S, Kallel S, Jmaiel M. How blockchain helps to combat trust crisis in COVID-19 pandemic? poster abstract. Paper presented at: Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys); Yokohama, Japan; 2020:764-765.
18. If you want to travel next year, you may need a vaccine passport; 2020 [Online]. https://edition.cnn.com/2020/12/27/tech/coronavirus-vaccine-passport-apps/index.html.
19. Benet J. Ipfs-content addressed, versioned, p2p file system; 2014. arXiv preprint arXiv:1407.3561.
20. Sporny M, Longley D, Chadwick D. Verifiable credentials data model 1.0. *W3C, W3C candidate recommendation*; March 2019.
21. ERC-1056 lightweight ethereum identity; 2018 [Online]. https://github.com/ethereum/EIPs/issues/1056.
22. JSON Web Tokens - JWT [Online]. https://jwt.io/. [Accessed: 15-Mar-2021].
23. Naik N, Jenkins P. uPort open-source identity management system: an assessment of self-sovereign identity and user-centric data platform built on blockchain. Paper presented at: Proceedings of the International Symposium on Systems Engineering (ISSE); Vienna, Austria; 2020:1-7; IEEE.
24. Infura Infrastructure Easily take blockchain application from testing to scaled deployment [Online]. https://infura.io/. [Accessed: 15-Mar-2021].
25. Next generation uPort identity app released; 2018 [Online]. https://medium.com/uport/next-generation-uport-identity-app-released-59bbc32a83a0.
26. Public-key authenticated encryption: crypto box; 2019 [Online]. http://nacl.cr.yp.to/box.html.
27. ERC-1098 encryption method; 2018 [Online]. https://github.com/ethereum/EIPs/pull/1098.
28. uPort project - Github repository; 2017 [Online]. https://github.com/uport-project.
29. TweetNaCl.js a high-level crypto library; 2018 [Online]. https://github.com/ethereum/EIPs/pull/1098.

30. NovidChain Proof of concept implementation; 2020 [Online]. https://github.com/amal-abid05/NovidChain.
31. Hicks C, Butler D, Maple C, Crowcroft J. SecureABC: secure AntiBody certificates for COVID-19; 2020. arXiv preprint arXiv:2005.11833.
32. Eisenstadt M, Ramachandran M, Chowdhury N, Third A, Domingue J. COVID-19 antibody test/vaccination certification: there's an app for that. *IEEE Open J Eng Med Biol*. 2020;1:148-155.
33. ETH Gas Station [Online]. https://ethgasstation.info/. [Accessed: 15-Mar-2021].
34. Shen J, Li Y, Zhou Y, Wang X. Understanding I/O performance of IPFS storage: a client's perspective. Paper presented at: Proceedings of the International Symposium on Quality of Service (IWQoS); Phoenix, Arizona, USA; 2019:1-10; IEEE.
35. Estonia, Hungary, and Iceland, together with AstraZeneca Estonia are participating in a pilot of Guardtime's VaccineGuard; 2021 [Online]. https://guardtime.com/blog/estonia-hungary-and-iceland-together-with-astrazeneca-estonia-are-participating-in-a-pilot-of-guardtime-s-vaccineguard.
36. COVI-Pass Tento health; 2020 [Online]. https://covipass.com/faq/.
37. DigiLocker Free, secure, flexible and easy-to-use application [Online]. https://digilocker.gov.in/. [Accessed: 15-Mar-2021].
38. Coronavirus: commission proposes a digital green certificate; 2021 [Online]. https://bit.ly/2Q2Z4ic.
39. IBM digital health pass; 2021 [Online]. https://www.ibm.com/products/digital-health-pass.
40. Mithani SS, Bota AB, Zhu DT, Wilson K. A scoping review of global vaccine certificate solutions for COVID-19; 2021.
41. Bansal A, Garg C, Padappayil RP. Optimizing the implementation of COVID-19 εimmunity certificatesε using blockchain. *J Med Syst*. 2020;44(9):1-2.
42. Mansour E, Sambra AV, Hawke S, et al. A demonstration of the solid platform for social web applications. Paper presented at: Proceedings of the International Conference Companion on World Wide Web (WWW); Montréal Québec Canada; 2016:223-226.
43. Groppe S. *Data Management and Query Processing in Semantic Web Databases*. Berlin, Germany: Springer Science & Business Media; 2011.
44. Tuli S, Mahmud R, Tuli S, Buyya R. FogBus: a blockchain-based lightweight framework for edge and fog computing. *J Syst Softw*. 2019;154:22-36.
45. Chen J, Hoops S, Marathe A, et al. Prioritizing allocation of COVID-19 vaccines based on social contacts increases vaccination effectiveness. *medRxiv*; 2021.
46. Tuli S, Tuli S, Tuli R, Gill SS. Predicting the growth and trend of COVID-19 pandemic using machine learning and cloud computing. *IoT*. 2020;11:100222.

How to cite this article: Abid A, Cheikhrouhou S, Kallel S, Jmaiel M. NovidChain: Blockchain-based privacy-preserving platform for COVID-19 test/vaccine certificates. *Softw Pract Exper*. 2021;1–27. https://doi.org/10.1002/spe.2983